Schaumburg Thoenes Thurn Landskron
New PCT Application
Case No. P05,0424 (26970-0398)
Client Ref. No. 2003-0701 PUS
Inventor: Jörgens et al.

Translation / 19 December 2005 / Bullock / 4780 words

METHOD AND DEVICE FOR PRINTING SENSITIVE DATA

The invention concerns a method and a device for printing of sensitive data.

Different methods are known for transmission of sensitive data to a printing device for printing of these data. For example, a system and a method in which an authorized person at a printing device must authenticate himself via input of a PIN before the respective printing process is executed arises from US 5,633,932. It is hereby assumed that the authorized person is present next to the printing device and can monitor the printing process during the printing process. The data to be printed are transmitted encrypted to the printing device and, as soon as the authentication has been effected by the authorized person, they are decrypted in the printer and stored in a print queue for processing. This method is very appropriate for small print jobs that are respectively monitored and executed by a specific person. When larger print jobs are executed at a printing device, the danger exists that an authorized person routinely authenticates himself without the necessary care being taken in the individual case. The function of the security device can hereby be eliminated. Additionally, the encrypted data are stored in a readable format in the print queue in the printing device, such that the printing device can be specifically manipulated and the sensitive data can be extracted.

A method similar to this is described in EP 1 091 285 A2, in which an authorized person has to authenticate himself at a printing device so that the print job is executed. The authentication hereby occurs by means of a smart card.

A printing device that comprises a decoder module with which coded data can be decoded or, respectively, decrypted arises from the US American [sic] patent application US 2001/0037462 A1. The encrypted data are transmitted to a driver device for printout on a recording medium. The driver device converts the decrypted print data into control signals for activation of a print head of the printing device.

In the printing of sensitive data such as, for example, the PIN for check cards or credit cards, a print file that contains the sensitive data is initially created and this file is encrypted. This process occurs in a security zone, i.e. in a hermetically sealed room on a computer system that can be separated from further networks during the operation, such that it is ensured that no unauthorized third parties can access the data to be processed. The print file so created is, for example, transferred onto a printing device with a data medium. The printout in turn occurs in a hermetically sealed room since, in the known printing devices, the encrypted data are decrypted and exist in a readable, decrypted form in the printing device. It is therefore necessary that, during the printing process, only a few authorized persons have access to the device and that the room in which the printing device is located is sealed. However, this also has the consequence that a print job with sensitive print data cannot simply be executed between two print jobs that merely contain non-sensitive data since extensive security measures must be taken for printing of the sensitive data. This applies even when the data are printed on a recording medium given which the printed data cannot be read after the printing process without destroying a casing or a seal or a corresponding other security mechanism. Such recording media are, for example, envelopes with an insert sheet that can be mechanically printed from the outside. Recording media with a security mechanism that makes a reading of sensitive data impossible without detectable alteration of the security mechanism is [sic] designated in the following as safety paper. Furthermore, safety paper is developed that can not just be mechanically printed but can also be printed with an electrophotographic printing device.

Since, in the known printing devices, the encrypted data is present in readable form in the printer, it is not possible to execute a print job of such sensitive data without hermetic sealing of the printing device.

A significant requirement exists for a printing device with which sensitive data can be printed without the printing device having to be hermetically sealed for printout of the data.

If sensitive data should be printed in large quantities, it is thus appropriate to use an electrophotographic printing device because corresponding high-capacity printers offer a high throughput, whereby every single page can be printed individually. In electrophotographic printers, a character generator is activated by means of a controller, which character generator exposes (with a laser or with light-emitting diodes) a photoconductor drum with which ink particles are transferred onto a recording medium. In "Das Druckerbuch – Technik und Technologien der OPS-Hochleistungsdrucker [sic], edition 5a, October 2000, ISBN-3-00-001019-X, such optical character generators are described in chapter 4 and a corresponding controller (the SRA controller) for activation of character generators is described in chapter 9. Raster techniques and their effect on the print quality are explained in chapter 6.

The invention is based on the object to achieve a method for printing of sensitive data given whose execution on a printing device it is not necessary to hermetically seal this printing device. Additionally, a device for execution of this method should be achieved with the invention.

The object is achieved via a method with the features of the claim 1 and via a device with the features of the claim 18. Advantageous embodiments of the invention are specified in the respective sub-claims.

The inventive method for printing of sensitive data comprises the following steps:

- encryption at a workstation of sensitive data to be printed,
- transfer to a printing device of the data to be printed,
- decryption of the sensitive data to be printed,

- conversion of the data to be printed into control signals for activation of a printing unit,
- printing of the data on a recording medium,

whereby the decrypted data are not stored in a readable format on a non-volatile storage medium between the decryption and the printing of the data.

Sensitive data in the sense of the present invention are all confidential or, respectively, secret data, in particular top secret data that are made accessible only to strictly limited personnel circles under significant security requirements.

A non-volatile storage medium in the sense of the present invention is any storage medium that retains the stored data over an unlimited time duration. In contrast to this, a volatile storage medium in the sense of the present invention is a storage medium that loses the data immediately as soon as the current feed of the storage medium is ceased.

Since, according to the invention, the data to be printed after the encryption are not stored in a readable format on a non-volatile storage medium, during the processing in a printing device the sensitive data are not present in a readable format. Even if it is sought during the printing process to manipulate the printing device such that it is halted, the sensitive data stored in the volatile memory are automatically deleted and, in the event that the sensitive data are stored on a non-volatile storage medium, they are stored in a non-readable format such that they cannot be read.

By non-readable form, what is understood in the sense of the invention is any format that cannot be read without further information that is inaccessible. For example, it is known that operating systems distribute certain data units in a fragmented manner in segments on a storage medium. However, these segments are only readable when the corresponding information for assembly of the segments exists. However, this information is inaccessible in most operating

systems since it is stored at a point unknown to the user. In the present invention, it is appropriate to store this information in a volatile memory such that, given a manipulation, this information is lost and the data stored on the non-volatile storage medium is no longer readable.

The invention thus makes it impossible to extract (via manipulation at the printing device) the data (supplied encrypted to the printing device from the printing device) during the working process of the decryption up to the printing on the recording medium. It is hereby no longer necessary to arrange the printing device in a hermetically-sealed room upon printing of sensitive data, and print jobs with sensitive data and print jobs with non-sensitive data that can be placed by any persons can be executed in series on the printing device.

The conversion of the data to be printed into control signals occurs in electrophotographic high-capacity printers for which the inventive method is provided via a known rastering of the data to be printed into raster images which represent the control signals for a character generator. In [sic] inventive method, the decryption of the sensitive data and the rastering of the same is [sic] advantageously executed in immediate succession, and the printing process is executed immediately following the rastering.

In a further preferred embodiment, sensitive and non-sensitive data are arranged mixed in a data unit (in particular a print file) before the transfer to the printing device, whereby the sensitive data are characterized by markings. It is hereby possible that the sensitive data can be processed independent of the non-sensitive data upon generation of a print file, such that, for example, an elaborate and extensive layout [sic] of any persons without security requirements can be created into which the sensitive data generated under high security requirements are then inserted in encrypted form. Since the data set of the sensitive data is normally significantly less in comparison to the data set of the non-sensitive data, the expenditure for the requirements of security can be kept low. This combination of

sensitive data and non-sensitive data in one printing unit represents an independent inventive idea.

The invention is subsequently, exemplarily explained in detail using the drawings. The drawings schematically show:

Fig. 1	a workstation and a printing device for execution of the inventive method,
Fig. 2	schematically, the design of a controller of the printing device from Fig. 1,
Fig. 3 – Fig. 6	respectively, schematically, an embodiment of the inventive method in a block diagram.

Fig. 1 shows a system for execution of the inventive method. This system comprises a printing device 1 that is connected with a workstation 2 via a data line 3.

A print file can be created at the workstation 2, which print file is conducted via the data line 3 to the printing device 1.

The printing device 1 comprises an input tray 4 to receive a stack of unprinted recording media and an output tray 5 in which printed recording media are stored. A transport path 6 for transport of the recording media is formed between the input tray 4 and the output tray 5. In Fig. 1, this transport path 6 is schematically shown and delimited by transport rollers 7. The recording media are conveyed in the transport direction 8 by means of the transport rollers.

A photoconductor drum 9 is arranged abutting on the transport path 6. The photoconductor drum 9 is exposed by means of an LED character generator and,

corresponding to the exposure of the photoconductor drum, ink particles are received by this at a developer station 11 and transferred onto the recording media. The character generator 10 is controlled by a control 12.

The character generator 10, the photoconductor drum 9 and the developer station 11 form a printing unit.

The printing device 1 is schematically shown roughly simplified in Fig. 1, whereby known elements that are necessary for the operation of the printing device (such as, for example, the fixer unit) have been omitted since they are without relevance for the invention.

A print file is generated at the workstation 2 and this print file is transferred to the printing device 1 via the data line 3. The print file is hereby, for example, transmitted in the form of a print data stream (for example IPDS, PDF, PS, PCL). The controller 12 receives the print data stream and executes a pre-processing in which the print data stream is converted into an intermediate language (for example meta-command list or, respectively, display list).

In the controller 12, the print data are converted into control signals for activation of the character generator 10. In electrophotographic high-capacity printers, this conversion of the print data occurs via a rastering, whereby the control signals are raster images whose pixels directly activate individual LEDs of the character generator 10.

On the input side, the controller 12 comprises an I/O module 14 for receipt of the print data. The I/O module 14 is coupled to a data bus such as, for example, the MultibusII® 15. Coupled to this data bus 15 are a decryption module 16 and one or more raster modules 17 as well as a print head data output 18 (that is also designated as a serializer). The raster module or, respectively, modules 17 and the print head data output 18 are connected with one another via a pixel bus 19 via

which the rastered print data are transferred. The rastered print data are forwarded to the character generator 10 at the print head data output 18.

A first embodiment of the inventive method is subsequently explained using Fig. 3.

Two data sets (data set 1 and data set 2) hereby exist, whereby the data of the one data set (data set 1) contain non-sensitive data and the data of the other data set (data set 2) contain sensitive data. The data set with the sensitive data is encrypted. Together both data sets form the print data.

The generation and processing of the data set containing the sensitive data occurs in a hermetically-sealed room. The data set is hereby also encrypted.

After the encryption, the data set containing the senstive [sic] data can be connected with the data set containing the non-sensitive data into print data [sic]. These print data are processed at the workstation 2 by means of a suitable application software (for example océ-Documentdesigner or a text processing program), whereby an application description or, respectively, a layout is initially worked out from the unencrypted data set, whereby regions are provided for accommodation of encrypted data that are marked by means of markings or commands. In principle, any type of command or marking can be used insofar as the markings/commands can be clearly interpreted in subsequent processing steps. In particular particular [sic] parameters, flags or tags, particular write commands and visible or non-visible identifiers (such as, for example, colors or fonts) are possible.

In the next processing step at the workstation 2, the print file is formatted on the basis of the application description and the available print data. This occurs by means of special formatters such as, for example, PRISMAproduction or océ-Windows-Application-Driver. It is hereby significant that the encrypted data are not decrypted but rather are inserted into the print file as encrypted data sets.

The generation of the print file thus on the one hand comprises the typical layout and text processing and the insertion of the encrypted data set into predetermined regions of the unencrypted data set. The encrypted regions are marked in the print file with suitable markers.

The print file in the form of a print data stream is forwarded to the printing device 1 via the data line 3.

Here the print data stream is received by the I/O module 14 of the controller 12 and fed into the data bus 15. The decryption module 16 reads the print data and detects the encrypted print data using the markings.

The encrypted print data are decrypted by the decryption module 16 at the request of the raster modules 17. The print data so decrypted are rastered by the raster modules 17 according to known raster techniques. The raster images hereby generated are forwarded to the print head data output 18 via the pixel bus 19.

The print head data output 18 forwards the raster image to the character generator 10 which controls (corresponding to the print data) the printing process onto a recording medium.

A recording medium in which the sensitive data cannot be read without destruction of a seal or envelope is advantageously used as a recording medium.

Alternatively, in the framework of the invention it is also possible to output the raster images in electronic form, for example as a file, e-mail, fax or the like. However, since they contain sensitive data, given such output it is necessary to encrypt them so that they can be forwarded to third parties.

In the above system, the decrypted data are present only in the region comprising the data bus 15, the pixel bus 19 and the data line between the print head data output 19 and the character generator 10. There is no non-volatile memory in this region. There is also no data unit between the decryption module 16 and the print head data output 18 that comprises and can read a data set containing larger, decrypted data.

The decryption module 16 stands in relationship to the raster modules 17 similar to the relationship of a coprocessor to a processor, meaning that the raster modules 17 transmit the encrypted information to the decryption module 16 for decryption and promptly retrieve the decrypted data again. The data are hereby not buffered but rather are converted by the raster modules into control signals for activation of a printing device.

In the printing device according to the present exemplary embodiment, the memory is virtually administered and each page is re-allocated as needed. The encrypted data and the decrypted control signals can therefore not be correlated even upon direct reading of the memory. The memory pages or, respectively, memory pages [sic] (that are normally 4 kilobytes in size) are administered by a separate program and are distributed on different raster modules. The corresponding linking information is not accessible from the outside. The format is machine-specific, meaning that it also cannot be interpreted without additional detailed knowledge. Additionally, no memory dump can be executed with the present embodiment of the printing device, meaning that the memory cannot be read by a third party. Additional software would have to be introduced for this. However, such interruptions and manipulations are registered by the controller.

It is thus not possible to arrive at the sensitive data via stopping the printing device and reading out the memory modules in this region. The memory modules of the raster module 17 respectively contain only segments of the print data, such that their association is practically impossible.

The decryption module 16 can be selected by the operator of the printing device himself and be added at a corresponding slot via insertion. Such decryption modules are typically designed such that they automatically self-destruct given mechanical interference. In the framework of the invention, it can also be appropriate to correspondingly design the raster modules 17 and the print head data output 18.

It can also be appropriate that the decryption module is to be activated by one or more keys, such that it is ensured that the printing device only prints sensitive data when one or more specific operators are physically present. These keys can, for example, be input at the printing device 1 via a control panel on the printing device or via a data medium such as, for example, a chip card.

Furthermore, it is appropriate to correspondingly identify safety paper inserted into the input tray 4 via an input on the control panel, whereby an operator may execute this only under prior authentication by means of a key. It is hereby ensured that sensitive data are only printed on corresponding recording media.

Alternatively, it is possible to provide a sensor to detect a corresponding safety paper on the transport path 6 in the region before the photoconductor drum 9, such that the printing process of sensitive data is automatically stopped if only a conventional recording medium should have been supplied to it.

In the above exemplary embodiment, a decryption module 16 and one or more raster modules 17 are provided. In the framework of the invention, it is also possible to link the calculations for decryption of the encrypted data with the calculations for rastering of print data and to execute them in a combined decryption/raster module.

The embodiment of the inventive method according to Fig. 4 essentially corresponds to that from Fig. 3. These differ merely in the design and in the formatting of the application. In the application description (layout), only the unencrypted data are considered. Corresponding blank areas are to be provided for the encrypted data.

These blank areas for the encrypted data can be generated via placeholders in order to be able to visualize the complete design. For this it is appropriate to use suitable markings. Additionally, the marking can also be used as a "positioning or formatting aid".

In the formatting of the application, the application is formatted on the basis of the application description (layout) and the available print data. This can be executed by means of special formatters such as, for example, PRISMAproduction or océ-Windows-Application-Driver.

In the embodiment of the inventive method according to Fig. 5, in comparison with the embodiment from Fig. 3 there are differences in the design of the print process and in the formatting and encryption of the application. In particular the data to be encrypted are only selectively encrypted after the generation of the print application or, respectively, print file.

In the application description (layout), the sensitive and the non-sensitive data are characterized by separate marking. In principle, any type of command or marking can be used insofar as it can be clearly interpreted in the next processing stages. In particular particular [sic] parameters, flags or tags, (write) commands or visible or non-visible identifiers (such as, for example, color or fonts) can be used for this.

The embodiment of the inventive method shown in Fig. 6 significantly corresponds to the embodiment shown in Fig. 5, whereby, however, neither commands nor markings for identification of the encrypted data are placed in the design of the

application and in the formatting of the application; rather, the entire application or, respectively, print files [sic] is encrypted.

The printing device used in the above embodiment is an electrophotographic high-capacity printer. Such high-capacity printers can print 400 DIN 4 pages per minute and more.

The invention can be summarized in brief according to the following:

The invention concerns a method and a device for printing of sensitive data.

According to the invention, the data are not held in a non-volatile memory after the decryption in the printing device; rather, they are immediately converted into control signals for activation of a printing unit and forwarded to the printing unit essentially without buffering.

It is hereby not possible to read the decrypted data via manipulation at the printing device.

Reference list

1	printing device
2	2 workstations
3	data line
4	input tray
5	output tray
6	transport path
7	transport OC [sic]
8	transport direction
9	photoconductor drum
10	LED character generator
11	developer station
12	controller
14	I/O module
15	data bus
16	decryption module
17	raster module
18	print head data output
19	pixel bus